

2018

춘계학술발표대회

논문집

일시 2018년 4월 27일(금) ~ 28일(토)

장소 제주대학교 아라캠퍼스 아라컨벤션홀

주최 사단법인 한국인터넷정보학회

주관 제주대학교

후원 네이버(주), (주)아이티센, (주)LGCNS,
(주)큐브시스템, LG히다씨(주), (주)워드바이스에세이리뷰



B-2-3	본질적 속성값을 이용한 한국어 감성사전 구축에 관한 실증연구	79
	류재관, 이건창(성균관대)	
B-2-4	스파크 분산 환경 기반 프라이버시 보호 빅 데이터 배포 시스템 개발	81
	김대호, 김태수, 유훈, 김종욱(상명대)	
B-2-5	Wasserstein CNN을 이용한 3D 물체 분류	83
	지명근, 전준철(경기대)	
B-2-6	★ 컨볼루션 신경망을 통한 2차원 키포인트 탐지 기반 3차원 인간 자세 추정 방법	85
	박서희, 지명근, 전준철(경기대)	
B-2-7	HMD를 활용한 가상현실 FPS게임 콘텐츠 개발	87
	이성진, 김민상, 홍민(순천향대)	
B-2-8	거리 정규화 레벨셋을 이용한 의료영상 분할	89
	윤희진, 지명근, 전준철(경기대)	

C-1. 인터넷보안 1 (좌장: 김문성 박사(특허청))

C-1-1	안드로이드 랜섬웨어 동향 분석	95
	서승희, 김역, 이창훈(서울과학기술대)	
C-1-2	CyberSecurity Framework와 ISO27001을 비교한 보안 통제 연구	97
	최중우, 원동호(성균관대)	
C-1-3	☆ 차세대 ITS 환경에서 익명성을 보장하기 위한 블록체인 활용 방안	99
	최석준, 곽진(아주대)	
C-1-4	최신 인증 암호화 기술의 안전성 분석	101
	조민정, 공성현, 이창훈(서울과기대)	
C-1-5	안드로이드 환경에서의 랜섬웨어 실시간 탐지 개선 방안에 관한 연구	103
	고주성, 곽진(아주대)	
C-1-6	사이버 레인지 훈련 지원 방안 연구	105
	김대식, 김용현(국방과학연구소)	

차세대 ITS 환경에서 익명성을 보장하기 위한 블록체인 활용 방안

최석준*, 곽진**

*아주대학교 컴퓨터공학과 정보보호응용및보증연구실

**아주대학교 사이버보안학과

e-mail : *sjchoi.isaa@gmail.com, **security@ajou.ac.kr

Using Block Chain to Ensure Anonymity in Cooperative ITS Environment

Suk-June Choi*, Jin Kwak**

*ISAA Lab., Department of Computer Engineering, Ajou University

**Department of Cyber Security, Ajou University

요 약

최근, 자율주행 차량 기술 발전으로 인해 운전자에 대한 편의성과 안전성을 높여줄 수 있는 기술 개발 연구가 활발히 진행되고 있다. 이러한 자율주행 기술을 제공하기 위해선 차량과 차량 간의 다양한 정보를 주고받아 해당 시스템을 구현한다. 하지만, 공격자에 의해 특정 차량에 대한 식별이 가능할 경우, 공격에 대상이 될 수 있으며, 이에 대한 안전성을 보장해주기 위해서는 차량에 대한 신원에 대한 추적을 할 수 없도록 해야 한다. 이를 위해 본 논문에서는 특정 차량에 메시지를 이용해 추적이 불가능 하도록 블록체인 시스템 환경을 적용하여 익명성을 보장할 수 있는 방안에 대한 연구를 진행한다.

1. 서 론

최근 4차 산업혁명을 중심으로 자율주행차량 기술에 대한 개발이 진행되고 있다. 자율주행차량 서비스가 구현되기 위해선 차량이 주고받는 통신에 대한 지연시간을 줄여야하지만, 메시지에 대한 안전성 확보가 이루어져야 한다. 만약 공격자에 의해 특정 차량에 대한 신원이 추적이 가능하게 된다면, 공격대상이 될 수 있으며, 서비스에서 주고받는 메시지에 대한 무결성, 기밀성 등을 보장해줄 수 없게 되며, 보안위협이 발생할 수 있다. 해당 문제를 해결하기 위해 기본적으로 차량 간 주고받는 메시지는 익명인증서를 통해 전자 서명을 하여 전송하게 된다. 이는 특정 차량에 대한 익명성을 보장해주면서, 동시에 정상적이지 않은 메시지에 대한 인증을 할 수 있다. 하지만, B.Wiedersheim에 연구에 따르면 익명인증서를 통해 차량이 메시지를 주고받는 경우에도, 공격자는 이를 분석하여 특정 차량에 대한 신원 추적 가능성에 대한 언급을 하고 있다[1].

따라서 본 논문에서는 차량에 대한 익명성을 보장해주기 위해 블록체인을 활용하는 방법에 대한 연구를 진행하고자 한다. 2장에서는 차량에서 익명성을 보장해주는 것이 가능한 블록체인의 트랜잭션 모델을 분석하며, 3장에서는 차량에서 블록체인을 적용 가능한 모델을 제안한다. 4장에서 결론을 맺는다.

2. 관련 연구

2.1 자율주행 차량 기술 단계

본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 대학ICT연구센터육성 지원사업의 연구결과로 수행되었음 (IITP-2018-2016-0-00304)

자율주행차량은 운전자의 편의성을 증대하기 위한 궁극적인 목표이며, 운전자가 차량을 직접 조작하지 않고 차량 내 시스템에서 도로상황 정보를 주고받아 운전자의 개입 없이 목적지까지 이동할 수 있게 해주는 기술을 말한다. SAE-J3016문서에 따르면, 자율주행 자동차 기술 단계는 0~5 Level까지 존재하며, 다음과 같다[2].

□ Human driver monitors the driving environment

자율주행 기술 단계 중 0,1,2 Level에 속하며 운전자가 운전 환경을 전부 수동으로 제어하는 수준이며, 부분적으로 운전 보조 시스템을 제공한다.

□ Automated driving system monitors the driving environment

자율주행 기술 단계 중 3,4,5 Level에 속하며 운전 환경을 부분적으로 자동 제어하는 수준이며, 최종 단계에서는 운전자의 개입 없는 완전한 자율 주행 단계를 말한다.

2.2 전통적인 블록체인 트랜잭션 모델의 문제점

전통적인 블록체인의 경우, 비트코인 주소 발행 시 입금에 대해 명확한 식별자가 함께 연결되고, 수신자의 가명과 연결된다. 이 경우 가명자의 공개키를 사용하기 때문에, 가명을 사용하더라도 특정 가명자의 트랜잭션에 대한 추적이 가능하여 익명성을 보장해줄 수 없다.

2.3 익명성 보장을 위한 블록체인 트랜잭션 모델 분석

일반적인 블록체인 기반 트랜잭션 모델은 특정 소유자에 대한 추적성이 존재한다. 따라서 차량에 대한 익명성을 보장해 주기 위해선, 표 1과 같이 가명 주소와 연결성을 없앤 방식의 트랜잭션 모델을 적용할 필요가 있다.

(표 1) 트랜잭션 모델 비교분석

트랜잭션 모델	공개키 방식	익명성 여부
전통적인 방식 (Bitcoin)[3]	가명자 공개키	익명성 보장 불가
Cryptonote 방식 (모네로)[4]	One-time 공개키	익명성 보장 가능

□ 전통적인 방식

가명자의 고유한 공개키를 사용하는 방식이기 때문에, 동일한 소유자에 대한 추적이 불가능하도록 하려면 트랜잭션마다 서로 다른 주소를 생성하고, 자신의 가명을 절대 사용하지 않아야 한다.

□ Cryptonote 방식

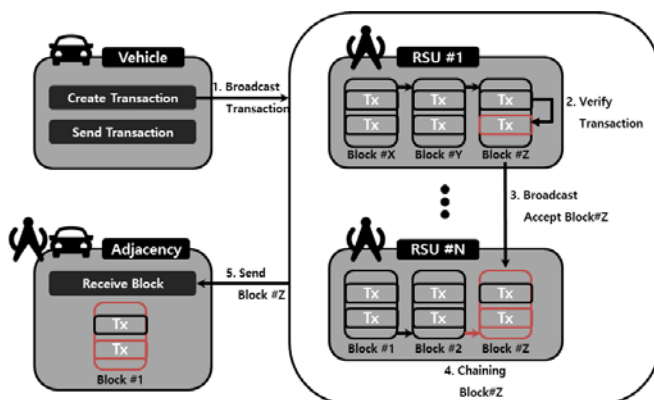
가명자의 고유한 공개키가 아닌 임의의 데이터에서 생성된 One-time 공개키 방식을 사용하기 때문에, 어떤 트랜잭션도 특정 주소로 보내지는지 연결성이 존재하지 않기 때문에 메시지에 대한 익명성 보장이 가능하다.

따라서 본 논문에서는 자율주행차량 환경에서 익명성을 보장해 주기 위해 Cryptonote 트랜잭션 모델을 적용한 블록체인을 활용한다.

3. 제안기법

3.1 블록체인을 적용한 차량 트랜잭션 방안

본 장에서는 자율주행차량 환경에서 차량에 대한 익명성을 보장해 주기 위한 익명성 보장 아키텍처를 제안한다. 제안하는 아키텍처는 블록체인 기반으로 각각의 메시지에 대한 검증을 진행하며, 특정 차량의 신원에 대한 익명성을 보장한다. 해당 아키텍처는 그림 1과 같다.



(그림 1) 익명성 보장을 위한 보안 아키텍처

□ Vehicle

자율주행차량은 도로상황의 정보를 주변 인접한 차량, RSU에게 보내기 위해 트랜잭션을 생성하고, 검증을 위해 RSU들에게 브로드캐스팅 한다.

□ RSU #1 ~ RSU #N

V2X 네트워크에 존재하는 RSU들은 블록체인을 생성하고, 트랜잭션에 대한 작업증명을 하는 검증자의 역할을 한다. 작업증명이 완료될 경우, 새로운 트랜잭션이 추가된 블록을 인접한 차량, RSU에게 전송한다.

□ RSU #1

RSU #1은 새로운 트랜잭션 Tx를 블록 Z에 추가하고, 블록에 대한 작업 증명을 진행한다. 해당 트랜잭션 검증 완료시 모든 노드에 블록 Z를 브로드캐스팅 한다.

□ RSU #N

RSU #N은 RSU #1으로부터 전달받은 블록 Z에 대한 블록 승인을 하기위해, 이전 해시로 승인된 블록 #2 뒤에 블록 Z를 연결한다. 이후 승인된 트랜잭션 메시지는 인접한 차량, RSU에게 브로드캐스팅 된다.

□ Adjacency

인접한 차량, RSU는 블록에 담긴 트랜잭션의 정보를 가지고 도로상황의 정보를 판단 및 처리한다.

4. 결 론

자율주행차량 환경에서는 차량 간 주고받는 메시지에 대한 안전성이 보장되어야 한다. 하지만, 익명인증서 체계의 경우, 신원을 추적 가능한 위협이 존재한다.

따라서 본 논문에서는 차량에 대한 익명성을 보장해 주기 위한 방법으로 블록체인을 활용하는 방안 연구를 수행하였다.

본 연구를 통해, 자율주행 차량환경에서 차량의 익명성을 보장해 주기 위한 방법으로 블록체인을 적용하기 위해선, 차량이 처리할 수 없는 블록체인 검증에 대한 방안, 사용되는 메시지를 트랜잭션에 전송하는 과정에 대한 검토 등의 추가적인 연구를 수행해야 하며, 향후 이를 통한 익명성 보장 아키텍처에 대한 검증, 분석 연구를 진행할 예정이다.

참 고 문 헌

- [1] B.Wiedersheim, F.Kargl, P.Papadimitratos, "Privacy in Inter-Vehicular Networks : Why simple pseudonym change is not enough", the 7th International Conference on Wireless On-demand Network Systems and Services, 2010.
- [2] SAE International, "SAE-J3016", 2014.
- [3] Nakamoto. S, "Bitcoin: A peer-to-peer electronic cash system", 2008.
- [4] Nicolas V. Saberhagen, "CryptoNote v 2.0", October 2013.